Reference 1

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平8－507416

(43)公表日　平成８年(1996)８月６日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ |
|---|---|---|---|
| Ｈ０４Ｌ　9/32 | | | |
| Ｇ０６Ｆ　15/00 | ３３０　Ｚ | 9364－5L | |
| Ｇ０９Ｃ　1/00 | | 7259－5Ｊ | |
| | | 8842－5Ｊ | Ｈ０４Ｌ　9／00　Ａ |

審査請求　未請求　予備審査請求　有　（全 36 頁）

(21)出願番号　特願平6－511416
(86)(22)出願日　平成５年(1993)11月２日
(85)翻訳文提出日　平成７年(1995)５月８日
(86)国際出願番号　ＰＣＴ／ＵＳ９３／１０５８５
(87)国際公開番号　ＷＯ９４／１０７７８
(87)国際公開日　平成６年(1994)５月11日
(31)優先権主張番号　９７０，６１１
(32)優先日　1992年11月３日
(33)優先権主張国　米国（ＵＳ）

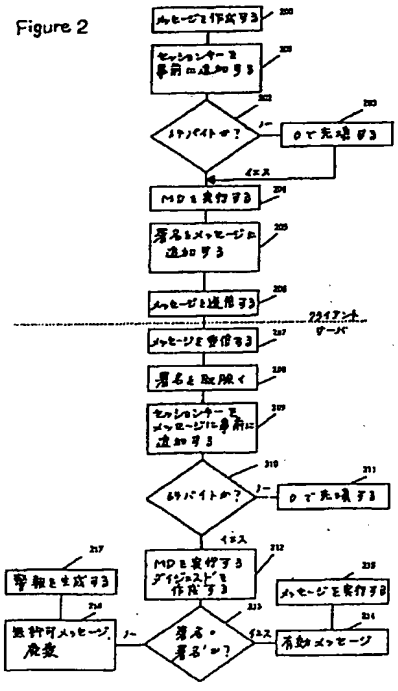
(71)出願人　ノーヴェル・インコーポレーテッド
アメリカ合衆国　84601　ユタ州・プロヴォ・イースト　1700　サウス・122
(72)発明者　キングドン，ケヴィン
アメリカ合衆国　84057　ユタ州・オーレム・イースト　600　ノース・1331
(74)代理人　弁理士　山川　政樹　（外５名）

最終頁に続く

(54)【発明の名称】　クライアントサーバ通信の認証のための方法及び装置

(57)【要約】
本発明は、メッセージパケットの偽造を防止するためのメッセージパケット認証の方法及び装置を提供する。そこで、署名と呼ばれるメッセージダイジェストの一部分を、実際のメッセージがワイヤを介して送信されるときに実際のメッセージに追加する（２０５）。受信局はメッセージから署名を取り除き（２０８）、同じ秘密セッションキーを事前に追加し（２０９）、それ独自のメッセージダイジェストを作成する（２１２）。受信局により作成されたダイジェストの署名を送信局により追加されたダイジェストの署名と比較する（２１３）。一致があれば、認証メッセージを想定する（２１４）。一致がなければ、メッセージを無効と考え、廃棄する（２１６）。

Figure 2



【特許請求の範囲】

１．センダとレシーバとの間で伝送されるメッセージを認証する方法において、前記センダでメッセージを生成する過程と；

前記メッセージとセッションキーを組合わせて、第１の追加メッセージを作成する過程と；

前記第１の追加メッセージの第１のダイジェストを計算する過程と；

前記第１のダイジェストの第１の部分を前記メッセージと組合わせて、送信メッセージを作成する過程と：

前記送信メッセージを前記レシーバへ送信する過程と；

前記送信メッセージから前記第１のダイジェストの前記第１の部分を取り除き、その結果として前記メッセージを得る過程と；

前記セッションキーを前記メッセージと組合わせて、第２の追加メッセージを生成する過程と：

前記追加メッセージの第１のダイジェストを計算する過程と；

前記第１のダイジェストの前記第１の部分と前記第２のダイジェストの第２の部分とを比較する過程と；

前記第１のダイジェストの前記第１の部分が前記第２のダイジェストの前記第２の部分と一致したときに前記メッセージを認証する過程とから成る方法。

２．前記センダはクライアント／サーバネットワークの中のクライアントである請求項１記載の方法。

３．前記レシーバはクライアント／サーバネットワークの中のサーバである請求項１記載の方法。

４．前記第１の追加メッセージの第１のダイジェストを計算する前記過程は、前記第１の追加メッセージについてダイジェストアルゴリズムを実行することにより実行される請求項１記載の方法。

５．前記ダイジェストアルゴリズムはＭＤ４ダイジェストアルゴリズムである請求項４記載の方法。

６．前記第１のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記センダの現在状態を初期状態として使用する請求項４記載

の方法。

７．前記第２のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記現在状態を初期状態として使用する請求項６記載の方法。

８．前記現在状態は認証されたメッセージが受信されるときに進む請求項７記載の方法。

９．前記現在状態は認証されたメッセージが受信されないときには進まない請求項８記載の方法。

１０．前記セッションキーは：

乱数列呼掛けを前記センダに対し実行する過程と；

前記センダのユーザからパスワードを要求する過程と：

前記パスワードから第１のパスダイジェストを生成する過程と；

前記第１のパスダイジェストと前記呼掛けをバッファにおいて組合わせる過程と；

前記バッファのバッファダイジェストを生成する過程と；

前記セッションキーを前記バッファダイジェストの第１の数のバイトとして定義する過程とにより生成される請求項１記載の方法。

１１．センダとレシーバとの間で伝送されるメッセージを認証する装置において、

前記センダでメッセージを生成する手段と；

前記メッセージとセッションキーを組合わせて、第１の追加メッセージを作成する手段と：

前記第１の追加メッセージの第１のダイジェストを計算する手段と；

前記第１のダイジェストの第１の部分を前記メッセージと組合わせて、送信メッセージを作成する手段と；

前記送信メッセージを前記レシーバへ送信する手段と；

前記送信メッセージから前記第１のダイジェストの前記第１の部分を取り除き、その結果として前記メッセージを得る手段と：

前記セッションキーを前記メッセージと組合わせて、第２の追加メッセージを生成する手段と；

前記第２の追加メッセージの第２のダイジェストを計算する手段と；

前記第１のダイジェストの前記第１の部分と、前記第２のダイジェストの第２の部分とを比較する手段と；

前記第１のダイジェストの前記第１の部分が前記第２のダイジェストの前記第２の部分と一致したときに前記メッセージを認証する手段とを具備する装置。

１２．前記センダはクライアント／サーバネットワークにおけるクライアントである請求項１１記載の装置。

１３．前記レシーバはクライアント／サーバネットワークにおけるサーバである請求項１１記載の装置。

１４．前記第１の追加メッセージの前記第１のダイジェストは、前記第１の追加メッセージについてダイジェストアルゴリズムを実行することにより計算される請求項１１記載の装置。

１５．前記グイジェストアルゴリズムはＭＤ４ダイジェストアルゴリズムである請求項１４記載の装置。

１６．前記第１のグイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記センダの現在状態を初期状態として使用する請求項１４記載の装置。

１７．前記第２のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記現在状態を初期状態として使用する請求項１６記載の装置。

１８．前記現在状態は認証されたメッセージが受信されたときに進む請求項１７記載の装置。

１９．前記現在状態は認証されたメッセージが受信されないときには進まない請求項１８記載の装置。

２０．セッションキーを生成する手段であって：

乱数列呼掛けを前記センダに対し実行する手段と：

前記センダのユーザからパスワードを要求する手段と；

前記パスワードから第１のパスダイジェストを生成する手段と；

前記第１のパスダイジェストと前記呼掛けとをバッファにおいて組合わせる手

段と；

前記バッファのバッファダイジェストを生成する手段と；

前記セッションキーを前記バッファダイジェストの第１の数のバイトとして定義する手段とを具備する手段をさらに含む請求項１１記載の装置。

【発明の詳細な説明】

# クライアントサーバ通信の認証のための方法及び装置

## 発明の分野

本発明はネットワーク通信の分野に関する。

## 背景技術

データ、アプリケーション、ファイル、処理パワー、通信並びにプリンタ、変復調装置、大容量記憶装置などの他の資源の共用を可能にするために、パーソナルコンピュータ又はワークステーションをコンピュータネットワークを介して連係できる。一般に、資源の共用はネットワークサーバの使用によって実行される。サーバは集中型資源を管理し、データを管理し、及び多くの場合に「クライアント」と呼ばれる他のＰＣやワークステーションとの資源を共用するのに専用に用いられる処理装置である。サーバと、ネットワークと、ＰＣ又はワークステーションとは、一体に組合わされて、クライアント／サーバコンピュータネットワークを構成する。クライアント／サーバネットワークモデルの１例を図１に示す。

図１は、サーバマシン１０２に結合するクライアントマシン１０１を示す。クライアントマシン１０１はＰＣ、ワークステーションなどであれば良い。サーバマシンは、ファイルを記憶する大容量記憶装置を含む専用プロセッサ、ＰＣ、ワークステーションなどであれば良い。典型的には、大容量記憶装置はディスクドライブ又は他の適切な装置である。

クライアントマシン１０１は、クライアントスタブ１０３と通信するクライアント１０２から構成されている。クライアントスタブ１０３はトランスポートエンティティ１０４と通信する。サーバマシン１０５はサーバ１０６と、サーバスタブ１０７と、トランスポートエンティティ１０８とを含む。

クライアントマシン１０１に関して説明すれば、クライアント１０２はサーバのファイルを利用する局所プロセッサである。クライアントスタブ１０３は、クライアントがサーバをアクセスすることを可能にする局所手続きの集合体である。トランスポートエンティティ１０４はネットワーク、すなわち、「ワイヤ」１０９に対するアクセスを実行する。ワイヤ１０９はクライアントとサーバとの間

の通信媒体を表わし、実際のハードワイヤード通信媒体であっても良く、あるいは、

無線接続であっても良い。同様に、サーバスタブ１０７はサーバがクライアントと通信することを可能にする手続きの集合体であり、トランスポートエンティティ１０８はサーバからワイヤ１０９へのアクセスを実行する。

動作中、クライアントとサーバとの通信は（クライアントからの）要求と（サーバからの）応答という形態をとる。この通信は遠隔手続き呼出しの形態である。クライアントは１つの手続きを呼出し且つ結果を獲得するアプリケーションに類似している。その相違点は、手続きが必ずクライアント１０１と同じマシンにあるとは限らず、むしろサーバマシン１０５にあるということである。

当初、クライアント１０２はクライアントマシンのクライアントスタブ１０３（クライアント１０２の局所アドレススペースに常駐している）にあるスタブ手続きを呼び出す。クライアントスタブ１０３はその呼出しからメッセージを構成し、メッセージをトランスポートエンティティ１０４に提供する。トランスポートエンティティ１０４はワイヤ１０９を介してメッセージをサーバマシン１０５へ通信する。サーバにおいては、トランスポートエンティティ１０８はメッセージをサーバスタブ１０７に渡す。そこで、サーバスタブはサーバ１０６から適切なサーバ手続きを呼び出す。サーバ１０６はメッセージに関して演算し、次にその手続きと何らかの結果をサーバスタブ１０７に戻す。サーバスタブ１０７は応答メッセージを構成し、それをトランスポートエンティティ１０８に提供する。応答メッセージはワイヤ１０９を介してクライアントマシン１０１のトランスポートエンティティ１０４へ送信される。トランスポートエンティティは応答メッセージをクライアントスタブ１０３に提供する。クライアントスタブ１０３は、サーバによって戻された手続きと何らかの値をクライアント１０２に戻す。

コンピュータネットワークでは、クライアントとユーザが異なる特権のレベルを有する。ユーザの追加、ユーザの削除、パスワードの変更などのいくつかの機能は最高の特権をもつユーザに限定されている。それらのユーザクライアントはネットワーク管理責任者であることが多く、それらのユーザは必要に応じてネッ

トワークを変更することが可能でなければならない。加えて、大半のユーザに対して制約が設けられているある種のファイル又はアクティビティもあるだろう。たとえば、金融データはその金融データを知る又は使用する必要があるユーザに限定されている場合が多い。一般に、他のユーザはそのデータをアクセスすることを許されない。

クライアント／サーバモデルにおいては、メッセージを「パケット」として転送する。メッセージパケットの１例を図３Ａに示す。メッセージは４バイトの長さヘッダー（ローハイ）標識３０１から構成されている。長さヘッダー３０１はその後に続くメッセージの長さを識別するもので、次のような情報を含む：

CheckSum

PacketLength

TransportControl

HPacketType

DestinationNet

DestinationNode

DestinationSocket

SourceNet

SourceNode

SourceSocket

長さヘッダー３０１の後に要求コード３０２が続く。要求コード３０２はクライアントによって要求されている手続きの特定の型である。要求コード３０２の後にデータ３０３が続く。データ３０３の長さは可変であっても良い。

メッセージパケットの特定の１つの型は「ＮＣＰパケット」と呼ばれるが、そのＮＣＰはＮｅｔＷａｒｅ　Ｃｏｒｅ　Ｐｒｏｔｏｃｏｌを表わしている。（ＮｅｔＷａｒｅはユタ州ＰｒｏｖｏのＮｏｖｅｌｌ，Ｃｏｒｐｏｒａｔｉｏｎの商標である）。ＮｅｔＷａｒｅはネットワークシステム用オペレーティングシステムである。ＮＣＰパケットは長さヘッダーの中に次の追加情報を含む：

packet type

sequence number

connection low

task

connection h igh

メッセージパケットの標準部分は発信元アドレスと、受信先アドレス及び長さとを始めとして、他の複数の情報を提供する。ＮＣＰ部分は接続番号と、シーケンス番号とを含む。ステーション接続番号は活動中のステーションのテーブルへの索引をサーバに与える。サーバは活動ステーションテーブルを使用し、そのステーションのネットワークアドレス及びシーケンス番号を含めた、ステーションのセッションに関する情報を追跡する。

接続番号は一部で機密性検査として使用される。サーバは、要求パケットを受信するときに、パケットの接続番号をその接続テーブルへの索引として使用する。要求パケットのネットワークアドレスは、その要求パケットに含まれている接続番号に対応する接続テーブルエントリに記憶されたネットワークアドレスと一致していなければならない。これは要求パケットを有効化する１つの方法である。

シーケンス番号もパケットを有効化するために使用される。シーケンス番号は、サーバとクライアントの双方によって維持されるバイトである。クライアントが要求パケットを送信するとき、そのクライアントはシーケンス番号を増分する。同様に、サーバは要求パケットを受信するときに、そのクライアントのシーケンス番号（サーバの接続テーブルに記憶されている）を増分する。シーケンス番号はクライアントによって２５６回目の要求が実行されるたびに（それが１バイトの長さであるために）循環する。

クライアントのシーケンス番号を増分する前に、サーバは既に受信した要求パケットのリストに照らしてシーケンス番号を検査する。この検査は、サーバが重複する要求パケットをサービスしないことを確認するためのものである。シーケンス番号が重複する要求パケットを指示しない場合、サーバはサーバの接続テーブルに記憶されているシーケンス番号に照らして要求パケットのシーケンス番号

を検査する。それら２つの番号が等しくなければ、サーバはパケットを廃棄する。

それらの予防措置にもかかわらず、時折、ネットワークアドレス、接続局、その局の接続番号及び局のシーケンス番号を検出することによるメッセージパケットの偽造の可能性はある。典型的には、メッセージパケットを偽造する目的は、偽造者の特権レベルを更新できるようにより高い特権をもつユーザ又はクライアントを「模倣する」ことである。偽造者は、通信媒体からネットワークパケットを捕捉することにより、さらに高い特権をもつ局の接続番号を捕獲できるであろう。それらは、より高い特権をもつ局からサーバへ送信されるネットワークパケットである。偽造者はプロトコル解析ツールを使用してそれらのパケットを捕獲しうるだろう。

接続番号を獲得することによって、偽造者は傍受されたメッセージの中と同じ局接続番号を使用して、メッセージをサーバ受信先アドレスへ送信することによりメッセージを偽造しようと試みるであろう。ところが、それだけでは侵入者がメッセージを偽造することを可能にするには不十分である。先に述べた通り、サーバはシーケンス番号を検査し、それを既に受信した要求のリストと比較する。新たな要求のシーケンス番号はそれと関連して、次に続くシーケンス番号を有しているべきである。有していないのであれば、それは無効の要求であり、サーバはそのパケットを廃棄する。

侵入者はシーケンス番号を「推測する」ことによりメッセージを偽造しようと試みるかもしれない。２５６の後にシーケンス番号は「循環する」ので、侵入者はシーケンス番号を見出す前に２５６回の試行を試みるだけで良い。侵入者はサーバからの応答を受信するのではなく、むしろ、サーバからの応答を検出しなければならないか又はサーバへ発行された要求が実行されているか否か（たとえば、侵入者に関わる特権状態の変化）を検出しなければならない。

ネットワーク侵入者に対して可能な解決方法の１つは、侵入者型アクティビティを検出するために使用されるネットワークを監視するというものである。たとえば、正しいシーケンス番号を提供するための試行錯誤の試みが検出されるよう

にネットワークを監視できるであろう。たとえば、シーケンス番号を提供するときのある回数の許容失敗試行を伴ってウィンドウを定義できるであろう。問題は、許容再試行のためのウィンドウの大きさに応じて、侵入者がそのウィンドウの中で無作為に正しいシーケンス番号を得ることもありうるという点である。ウィンドウを小さくすれば、正当なユーザが正しいシーケンス番号を与えないときに正当なトランザクションが中断されてしまうであろう。侵入者のアクセスを単に検出する代わりに、侵入者のネットワークアクセスを防止する方法及び装置を提供することが望まれる。

## 本発明の概要

本発明は、メッセージパケットの偽造を防止するためのメッセージパケット認証の方法及び装置を提供する。メッセージパケットを作成した後、そのメッセージに秘密セッションキーを事前に追加し、変更したメッセージについてメッセージダイジェスティングアルゴリズムを実行して、メッセージダイジェストを作成する。次に、署名で呼ばれるメッセージダイジェストの一部分を、実際のメッセージがワイヤを介して送信されるときに実際のメッセージに追加する。受信局はメッセージから署名を取り除き、同じ秘密セッションキーを事前に追加し、それ独自のメッセージダイジェストを作成する。受信局により作成されたダイジェストの署名を、送信局により追加されていたダイジェストの署名と比較する。一致があれば、認証メッセージを想定する。一致がないならば、メッセージを無効と考え、廃棄する。本発明の１つの利点は、セッションキーが決してワイヤを介して送信されないことである。受信局（サーバ）は既にキーをもっており、キーをメッセージデータと共に使用して、パケットを受信した時点でメッセージダイジェストを再計算する。ＮＣＰセッションの開始中に共用秘密キー（セッションキー）を生成する。加えて、送信局と受信局の双方により累積状態情報を維持しておく。この状態情報もメッセージを認証するために使用される。

## 図面の簡単な説明

図１は、クライアント／サーバモデルのブロック線図である。

図２は、本発明のセッションキーを使用するメッセージセッションの流れ図で

ある。

図３Ａ～図３Ｇは、メッセージセッション中のメッセージ構造の図である。

図４は、メッセージセッション中のクライアント状態の流れ図である。

図５は、メッセージセッション中のサーバ状態の流れ図である。

図６は、セッションキーの生成を示す流れ図である。

図７は、セッションキーを認証する方法の流れ図である。

図８は、本発明を実現しうるコンピュータシステムのブロック線図である。

図９は、本発明のブロック線図である。

## 発明の詳細な説明

メッセージ認証の方法及び装置を説明する。以下の説明中、本発明をさらに完全に理解させるために、メッセージ型、メッセージ長さなどの特定の詳細な事項を数多く挙げる。しかしながら、それらの特定の詳細がなくとも本発明を実施しうることは明白であろう。別の場合には、本発明を無用にわかりにくくしないように周知の特徴を詳細には説明していない。

本発明はメッセージごとに、センダを識別し且つ認証する署名を与える。さらに、本発明はセッションに関する状態情報を追跡し、その累積効果を使用して、センダを保護し且つ認証するのを助ける。

本発明の署名方式は「メッセージダイジェスティング」として知られている動作を利用する。メッセージダイジェスティングはデータの保全性を与え且つ誤りを検出するための方式である。使用に際して利用可能なメッセージダイジェスティングアルゴリズムはいくつかあり、そのいくつかはＲｉｖｅｓｔ，Ｓｈａｍｉｒ及びＡｓｓｏｃｉａｔｅｓ（ＲＳＡ）により提供されている。ＲＳＡメッセージダイジェスティングアルゴリズムはＭＤ２，ＭＤ４及びＭＤ５として知られている。本発明の好ましい実施例は、メッセージダイジェスティングアルゴリズムＭＤ４から派生したものを利用する。ＭＤ４アルゴリズムは、本明細書にも参考として取り入れられているＲＦＣ１３２０「Ｔｈｅ　ＭＤ４　Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ」，Ｒ．Ｒｉｖｅｓｔ，ＭＩＴ　Ｌａｂｏｒａｔｏｒｙ　ｆｏｒ　Ｃｏｍｐｕｔｅｒ　Ｓｃｉｅｎｃｅ　ａｎｄ　ＲＳＡ　Ｄ

ａｔａ　Ｓｅｃｕｒｉｔｙ，Ｉｎｃ．１９９２年４月の中で説明されている。本発明の好ましい実施例では、ＭＤ４アルゴリズムの中で説明されているパディング方式の代わりに、ここで説明するパディング方式を使用する。しかしながら、本発明はどのような適切なパディング方式と組み合わせても使用可能であろう。加えて、ＭＤ２ダイジェスティングアルゴリズムやＭＤ５ダイジェスティングアルゴリズムをダイジェスティングアルゴリズムとして使用しても良い。

ダイジェスティングアルゴリズムの代わりに、本発明の趣旨から逸脱することなく、他の暗号の上で安全である一方向ハッシングアルゴリズムを使用しても良い。ハッシュ関数は、値を広い定義域からより小さな範囲にマッピングする数学的関数である。好ましい実施例では、ハッシュ関数はその関数を定義域内の１組の値に適用した結果がその範囲にわたって一様に（且つ見かけは無作為に）分布するようなものである。この方式を使用すると、時間を節約しつつ、依然として有効なデジタル認証署名の利点を発揮するように、メッセージの暗号化を回避することができる。

メッセージ署名

メッセージを認証するために署名を作成し且つ利用する方法を図２の流れ図に示す。ステップ２００では、クライアントによりメッセージを作成する。このメッセージは図３Ａに示すようなものである。メッセージは４バイトの長さヘッダー（ローハイ）標識３０１から構成されている。長さヘッダー３０１はその後に続くメッセージの長さを識別し、発信元と受信先の情報を含む。長さヘッダー３０１の後に要求コード３０２が続く。要求コード３０２は、クライアントにより要求されている特定の型の手続きである。要求コード３０２の後にデータ３０３が続いている。データ３０３の長さは可変であっても良い。

ステップ２０１では、以下に詳細に説明するようにして作成されるセッションキーをメッセージに事前に追加する。図２のステップ２０１のセッションキーの事前追加を図３Ｂに示す。８バイトのキー３０４は長さ標識３０１の前でメッセージに事前追加される。

決定ブロック２０２では、引き数「６４バイトか？」を形成する。引き数が偽

である場合、すなわち、メッセージが６４バイトを有していない場合、システムはステップ２０３へ進み、メッセージの残り部分を零で充填する。これは図３Ｂのパディング３０５である。好ましい実施例においては、必要に応じてパディング３０５（複数の零から構成されている）がメッセージの終わりに追加されるように、メッセージダイジェストアルゴリズムは演算に際して６４バイトを要求する。要求コードとデータを合わせて６４バイトであり、４バイトの長さは合わせて６４バイトに対してセッションキーの８ビットの中で指示されている。

ステップ２０３の後、すなわち、決定ブロック２０２における引き数が真であれば、システムはステップ２０４へ進む。ステップ２０４では、事前追加メッセージからメッセージダイジェストを生成するためにメッセージダイジェストアルゴリズムを実行する。メッセージダイジェストアルゴリズムの実行は図３Ｃの１６バイトのメッセージダイジェストを作成する。

ステップ２０５では、ダイジェストの初めの８バイト、すなわち、署名３０６をメッセージに追加する。これを図３Ｄに示す。８バイトの署名３０６は実際のＮＣＰデータの終わりに追加される。メッセージをワイヤを介して送信するにはパディングは不要である。ステップ２０６では、メッセージをサーバへ送信する。ステップ２００～２０６はクライアントにより実行され、ステップ２０６～２１６はサーバにより実行される。

ステップ２０７でサーバはメッセージを受信する。ステップ２０８でサーバはメッセージから署名３０６を取り除く。署名３０６は図３Ｅに示すようにメッセージから取り除かれる。

ステップ２０９では、サーバはサーバによって生成、記憶されていたセッションキー（有効ユーザにより生成、記憶されたのと同じセッションキーであるべきである）をメッセージに事前追加する。メッセージにサーバ側セッションキー３０４′が事前追加されている図３Ｆに示されている。決定ブロック２１０では、引き数「６４バイトか？」を形成する。引き数が偽であれば、システムはステップ２１１へ進み、図３Ｆのパディング３０５により示すように、メッセージの残る部分を零によって充填する。

ステップ２１１の後、すなわち、決定ブロック２１０における引き数が真である場合には、システムはステップ２１２へ進む。ステップ２１２では、ＭＤ４アルゴリズムを実行して、ここではダイジェスト′と呼ばれるサーバメッセージダイジェストを作成する。この結果、図３Ｇの１６バイトのメッセージダイジェストが得られる。このメッセージダイジェストの初めの８つのバイト、すなわち、署名′３０６′も次に取り除き、クライアントによりメッセージと共に送信されていた署名３０６と比較する。

決定ブロック２１３では、引き数「署名＝署名′か？」を形成する。このステップは、クライアントにより生成された署名がサーバにより生成された署名′と同じであるか否かを判定するためのものである。決定ブロック２１３における引き数が真であれば、システムはステップ２１４へ進み、有効メッセージが示される。ステップ２１５では、そのメッセージを実行する。決定ブロック２１３における引き数が偽であれば、システムはステップ２１６へ進む。ステップ２１６では、無許可メッセージを指示し、そのメッセージを廃棄する。ステップ２１７では、無許可メッセージが試みられたことを指示するために警報を生成する。

本発明の好ましい実施例はダイジェストの８つのバイトを署名として利用する。署名としては、本発明の範囲から逸脱することなく、ダイジェストの任意の数のバイト又はビットを使用して良い。

場合によっては、メッセージパケットは８バイトのメッセージダイジェストを追加する能力を除外して、データフィールド全体を使用する。典型的なアプリケーションにおいては、ブロックサイズ折衝はプロトコルヘッダー情報に対して６４バイトを想定する。現実には、大半のプロトコルヘッダーが消費するバイトは５６バイト未満であるので、８バイトのダイジェスト情報のために常に利用可能な８つのバイトが残される。８バイトの空きスペースを利用できなければ、８バイトのスペースを保証できるように人為的により小さくしたブロックサイズを折衝する。

状態追跡

先に説明したメッセージ署名方式に加えて、本発明は状態情報を使用するメッ

セージ認証の方法をも提供する。ＭＤ４アルゴリズムは、それが累積的である、すなわち、メッセージダイジェスト機能を複数の段で実行できるような性質のものである。

たとえば、メッセージのファイルの１つのブロックをメッセージダイジェストアルゴリズムに提供して、ダイジェスティングすることができ、ファイルの次のブロックを読込み、ダイジェスティングを継続して行くことができる。ダイジェスティングアルゴリズムの実行の出力状態は次のダイジェスティングステップにおける入力状態として使用される。複数の段におけるメッセージダイジェストアルゴリズムを実行することの正味の効果は、メッセージダイジェストアルゴリズムが情報の１ブロック全体を１回のパスで実行するかのようなものである。すなわち、その都度のアルゴリズム実行の終了時の状態を覚えておくことによって、累積効果が得られる。本発明はこの累積効果と状態情報を利用して、追加レベルの機密保護と認証を与える。

クライアントとサーバは共に状態情報を追跡し且つ記憶する。本発明では、この状態情報は最も近い時点で生成されたメッセージダィジェストから構成されている。現在メッセージダイジェストと新たなメッセージを使用して、仮メッセージダイジェストがクライアント及びサーバによって生成、記憶される。新たなメッセージが受信されると、新たなメッセージダイジェストを生成して、仮ダイジェストと比較する。他方の相手方が先行状態情報を有していた場合に限って一致が可能である。正しくない開始状態情報は、侵入者と偽造メッセージを識別する誤りを伝搬させる。

図４を参照すると、クライアントに関わる状態追跡の流れ図が示されている。ステップ４０１では、クライアントの現在状態は先の有効メッセージから生成された全１６バイトのメッセージダイジェストである。ステップ４０２では、クライアントは新たなメッセージを生成する。ステップ４０３では、現在状態（ダイジェスト）を仮状態を作成するための開始点として使用して、クライアントはメッセージダイジェスティングアルゴリズムを新たなメッセージに適用する。

ステップ４０４では、メッセージをサーバへ送信する。ステップ４０５では、

クライアントはサーバからの応答を受信する。ステップ４０６では、ステップ４０３の仮状態を使用して、その応答を検査する。これは、メッセージからサーバ側で生成されたダイジェストを取り除き、（開始点として仮状態を使用して）メッセージダイジェストアルゴリズムをメッセージに適用し、その結果得られたダイジェストの初めの８つのバイトをサーバ側で生成されたダイジェストの初めの８つのバイトと比較することによって実行される。

決定ブロック４０７では、引き数「有効応答か？」を形成する。引き数が偽であれば、システムはステップ４０８へ進み、無効応答が受信されているために状態を進ませない。クライアントにより生成される次のメッセージは、ダイジェスティングアルゴリズムに関わる開始点として既存の現在状態を使用する。決定ブロック４０７における引き数が真であれば、システムはステップ４０９へ進み、状態を進ませる。すなわち、仮状態を現在状態にする。ダイジェスティングアルゴリズムを次のメッセージに適用するとき、その新たな現在状態は開始点となる。

場合によっては、クライアントはデータのバーストをサーバへ送信するかもしれないし、あるいは、クライアントはバースト応答を生成するかもしれない。（第１のパケットを除き）パケットバースト中のメッセージの順序は必ずしも固定していない。ダイジェスティングアルゴリズムが累積的な性質であるため、これによって状態情報の計算時に問題を引き起こす可能性がある。パケットバースト応答に対して、サーバは第１の応答パケットについてメッセージダイジェストを計算し、同じ状態を使用して、バースト中の残る全てのパケットについてメッセージダイジェストを計算する。このように、第１のパケットの後のパケットの順序にかかわらず、状態の保全性を維持できるのである。

バースト要求は同様に処理される。ストリーム中の第１のパケットはダイジェストアルゴリズムの状態でくくり出しされる。バースト要求の中の後続パケットは初期状態として第１のパケットと同じ状態を使用する。

状態情報を維持するときのサーバの動作を表わす流れ図を図５に示す。ステップ５０１では、サーバはクライアントからのメッセージを受信する。決定ブロッ

ク５０２では、引き数「バーストか？」を形成する。引き数が真であれば、システムは第１のパケットの状態を使用し、ステップ５０３に戻る。引き数が偽であれば、システムはステップ５０３へ進み、シーケンス番号を検査する。決定ブロック５０４では、引き数「繰返しシーケンス番号か？」を形成する。これは繰返し要求を識別するためのものである。要求パケットに対して生成されたダイジェスト出力は常にダイジェスト状態へくくられる。すなわち、繰返し要求が現れたときには、サーバにより先のダイジェスト状態を維持しなければならないのである。決定ブロック５０４における引き数が真であれば、システムはステップ５０５へ進み、新たなメッセージに基づき、記憶されていた先行状態を使用して仮状態を再計算する。

決定ブロック５０６では、引き数「バーストか？」を形成する。引き数が真であれば、システムは第１のパケットの状態を使用するステップへ進み、ステップ５０７に戻る。引き数が偽であれば、システムはステップ５０７へ進む。ステップ５０７では、仮状態に基づいてメッセージの署名を検査する。決定ブロック５０８では、引き数「有効か？」を形成する。引き数が偽であれば、システムはステップ５０９でメッセージを廃棄し、偽造のおそれのあるメッセージに関して警報を発生する。決定ブロック５０８における引き数が真であれば、ステップ５１０でシステムはメッセージに対し応答する。

決定ブロック５０４における引き数が偽であれば、システムは決定ブロック５１１へ進む。決定ブロック５１１では、引き数「次に連続するシーケンス番号か？」を形成する。引き数が偽であれば、システムはステップ５１２へ進み、メッセージを無効と宣言し、それを廃棄する。言いかえれば、シーケンス番号は不適切だったのである。決定ブロック５１１における引き数が真であれば、システムはステップ５１３へ進み、維持されていた仮状態に基づいて署名を検査する。

決定ブロック５１４では、引き数「有効か？」を形成する。引き数が偽であれば、システムはステップ５０９へ進み、メッセージを廃棄し、且つ警報を生成する。引き数が真であれば、システムはステップ５１５へ進む。ステップ５１５では、仮状態を現在状態として再定義する。ステップ５１６では、応答に基づいて

新たな仮状態を作成する。決定ブロック５１７では、引き数「バーストか？」を形成する。引き数が真であれば、システムは第１のパケットの状態を使用し、ステップ５１８へ進む。引き数が偽であれば、システムはステップ５１８へ進み、計算されていた仮状態に基づいてクライアントに応答する。

セッションキー

クライアントセッションキーを生成する方法を図６に示す。ユーザがネットワークを介して通信することを試みるとき、まず、サーバに対してユーザを識別しなければならない。セッションを開始するために、ユーザはクライアントマシンにログオンしようとする。ステップ６０１では、クライアントはサーバマシンからの呼掛けを要求する。呼掛けは８バイト分の乱数から構成されている。そこで、クライアントは、ステップ６０２で、ユーザに対してアカウント名とパスワードを求める。ユーザがアカウント名とパスワードを入力すると、クライアントマシンはステップ６０３でそのアカウントと関連するオブジェクトＩＤを確定する。（オブジェクトＩＤは、各アカウントと関連する数字代理キー、すなわち、索引である。）

ステップ６０４では、クライアントマシンはパスワードとオブジェクトＩＤを使用して、ここではＤｉｇｅｓｔ１と呼ばれる１６バイトの結果を生成するためにダイジェストアルゴリズムを使用してダイジェストを計算する。ステップ６０５では、クライアントマシンはＤｉｇｅｓｔ１と、呼掛けと、オプションとしてのテキストストリングとのバッファを構成する。好ましい実施例では、本発明のテキストストリングは「許可ネットウェアクライアント」である。ダイジェストアルゴリズムの実行に際して６４のバイトを形成するために、必要に応じてバッファに０をパディングする。

ステップ６０６では、Ｄｂｕｆｆｅｒと呼ばれるバッファのダイジェストを生成するために、クライアントマシンはバッファについて第２のダイジェスト（Ｄｉｇｅｓｔ１、呼掛け、０のパディング及びオプションとしてのテキストストリング）を実行する。ステップ６０７の後、Ｄｂｕｆｆｅｒの初めの８つのバイトを取り除き、セッションキーとして定義する。本発明の好ましい実施例ではセッ

ションキーとして8バイトを使用するが、本発明の範囲から逸脱することなく任意の数のバイト又はビットを使用して良い。

サーバはユーザのパスワードと、アカウント名と、オブジェクトＩＤをも記憶している。サーバは呼掛けをも生成しており、その値を記憶する。サーバマシンは同一のステップを使用して、セッションキーを生成することができる。すなわち、セッションキーがワイヤを介して送信されることは決してない。それはクライアントマシンとサーバマシンにおける機密情報から生成される。加えて、セッションキーは１つには呼掛け（乱数）によって決まるので、セッションキーはクライアント／サーバセッションごとに異なる。

図６には示されていないが、呼掛けに対して応答はステップ６０４の後で生成される。ワイヤを介してサーバへ送信される応答は、ステップ６０５及び６０６で使用されるハッシングアルゴリズムとは異なるハッシングアルゴリズムによって生成される。ＭＤ４アルゴリズムを使用してステップ６０４を実行する場合には、呼掛け応答は、たとえば、ＭＤ５アルゴリズムを使用でき、セッションキーはＭＤ４アルゴリズムを使用して生成される。あるいは、ＭＤ４アルゴリズムを使用して呼掛け応答を生成することができ、ＭＤ５アルゴリズムなどの異なるアルゴリズムを使用してセッションキーを生成することが可能である。一方のアルゴリズムの出力から他方のアルゴリズムの出力へのマッピングがない限り、別の

どのようなダイジェスティング方式又はハッシング方式でも使用できる。

ＭＤ５アルゴリズムは、本明細書に参考として取り入れられているＲＦＣ１３２１，「Ｔｈｅ ＭＤ５ Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ」，Ｒ．Ｒｉｖｅｓｔ，ＭＩＴ Ｌａｂｏｒａｔｏｒｙ ｆｏｒ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ ａｎｄ ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ，Ｉｎｃ．１９９２年４月の中に説明されている。

セッションキー認証

図７は、セッションキーを認証する方法の流れ図を示す。ステップ７０１では、クライアントは図６に関連して説明したようにしてセッションキーを生成する。ステップ７０２では、図２に関連して説明したようにダイジェストと署名を生

成するためにセッションキーを使用して、クライアントによりサーバへ要求を送信する。

ステップ７０３では、サーバはクライアントのメッセージから署名を取り除き、サーバ側に記憶されているアカウント名、パスワード及びオブジェクトＩＤのコピーを使用して、まず、そのＤｉｇｅｓｔ１のバージョン、すなわち、Ｄｉｇｅｓｔ１′を生成し、次にＤｉｇｅｓｔ１′を使用して、セッションキーのサーババージョン、すなわち、セッションキー′を生成する。ステップ７０４では、サーバは図２に関連して説明したようにＤｉｇｅｓｔ′を生成する。

決定ブロック７０５においては、引き数「署名＝署名′か？」を形成する。引き数が偽であれば、システムはステップ７０６へ進み、サーバは否定のａｃｋ（応答）をクライアントへ送信し、サーバはその状態を変えない。サーバは新たなセッションに際してその状態を初期設定しない。決定ブロック７０５における引き数が真であれば、システムはステップ７０７へ進み、サーバは「ＯＫ」の肯定応答をクライアントへ送信する。ステップ７０８では、サーバはクライアント状態を初期設定し、サーバが生成したセッションキーを記憶する。ステップ７０９では、サーバはサーバ状態を初期設定し且つセッションキーを記憶する。クライアントとサーバの初期状態は、たとえば、ＭＤ４規格で文書化されている初期状態であるとして定義される。

本発明のクライアント及びサーバは任意の従来通りのコンピュータシステム又は汎用コンピュータシステムで実現されれば良い。本発明を実現するためのコンピュータシステムの一実施例の一例を図８に示す。キーボード８１０及びマウス８１１は両方向システムバス８１８に結合している。キーボードとマウスはコンピュータシステムにユーザ入力を導入し且つそのユーザ入力をＣＰＵ８１３へ通信するためのものである。図８のコンピュータシステムはビデオメモリ８１４と、主メモリ８１５と、大容量記憶装置８１２とをさらに含み、それらは全てキーボード８１０、マウス８１１及びＣＰＵ８１３と共に両方向システムバス８１８に結合している。大容量記憶装置８１２は、磁気記憶システム、光学記憶システム又は磁気光学記憶システム、あるいは他の何らかの利用可能な大容量記憶技術

などの固定媒体と着脱自在な媒体の双方を含んでいて良い。バス８１８は、たとえば、ビデオメモリ８１４又は主メモリ８１５をアドレス指定するためのアドレス線を３２本含んでいても良い。システムバス８１８は、たとえば、ＣＰＵ８１３、主メモリ８１５、ビデオメモリ８１４及び大容量記憶装置８１２などの構成要素の間でデータを転送する３２ビットデータバスをさらに含む。あるいは、別個のデータ線とアドレス線の代わりに、多重データ／アドレス線を使用しても良い。

本発明の好ましい実施例では、ＣＰＵ８１３はＩｎｔｅｌによって製造されている８０３８６又は８０４８６などの３２ビットマイクロプロセッサである。しかしながら、他の何らかの適切なマイクロプロセッサ又はマイクロコンピュータを利用しても良い。主メモリ８１５はダイナミックランダムアクセスメモリ（ＤＲＡＭ）から構成されている。ビデオメモリ８１４はデュアルポートビデオランダムアクセスメモリである。

ビデオメモリ８１４の一方のポートはビデオ増幅器８１６に結合している。ビデオ増幅器８１６は陰極線管（ＣＲＴ）ラスタモニタ８１７を駆動するために使用される。ビデオ増幅器８１６は当該技術では良く知られており、何らかの適切な手段によって実現されれば良い。この回路はビデオメモリ８１４に記憶されている画素データをモニタ８１７により使用するのに適するラスタ信号に変換する。モニタ８１７は図形画像を表示するのに適する種類のモニタであり、本発明の好ましい実施例においては、約１０２０×８３２の分解能を有する。本発明では他の分解能のモニタを利用しても良い。

以上説明したコンピュータシステムは単なる例示を目的としている。本発明はどのような種類のコンピュータシステム、あるいはプログラミング環境又は処理環境でも実現されうるであろう。

本発明のブロック線図を図９に示す。メッセージ発生器９０１は送信局から受信局に至るメッセージの供給源である。この例では、送信局はクライアントであり、受信局はサーバである。メッセージ発生器９０１はメッセージ９０２を提供する。セッションキー９０４はセッションキー記憶装置９０３に記憶されている

。セッションキー９０４は加算器９０５でメッセージ９０２に事前追加され、その結果として追加メッセージ９０６を得る。追加メッセージ９０６はダイジェスタ／バッファブロック９０７に供給されて、そこでダイジェスティングされ、その初めの８つのバイトを署名９０８として使用する。署名９０８は加算器９１１でメッセージ９０２と組合わされ、その結果として署名付きメッセージ９１２を得る。署名付きメッセージ９１２は送受信機９１３を介して受信局に結合される。

状態記憶装置９０９は受信局の現在状態と仮状態を記憶しており、それらを線路９１０を介して必要に応じてダイジェスタ／バッファブロック９０７に供給する。セッションの初期設定時にセッションキー９０４を生成するために、呼掛け９２３と局所パスワード９２４もダイジェスタ／バッファブロック９０７に提供される。

受信後の署名付きメッセージ９１４は減算器９１５で署名９１６及びメッセージ９１７という要素に分離される。メッセージ９１７は加算器９１８でセッションキー記憶装置９１９からのセッションキー９２０と組合わされ、その結果として追加メッセージ９２１を得る。追加メッセージ９２１はダイジェスタ／バッファ９２２に提供され、そこでダイジェスティングされる。ダイジェストの初めの８つのバイトは署名９２７を定義する。署名９２７は、受信メッセージ９１４の署名９１６と共に、比較／認証ブロック９２８に提供される。比較／署名ブロックは署名９２７を署名９１６と比較する。署名が一致したとき、有効メッセージを指示する。署名が一致しない場合には、メッセージは無効であると宣言し、メッセージを廃棄する。

ダイジェスタ／バッファ９２２のダイジェスティング動作のための状態情報は状態記憶装置９２５から線路９２６を介して提供される。呼掛け９２９とパスワード９３０も、セッションキーの生成のために、ダイジェスタ／バッファ９２２に提供される。

図９の要素は処理手段における実行可能な命令として実現可能である。

以上、クライアント／サーバ通信の認証のための方法及び装置を説明した。

【図１】

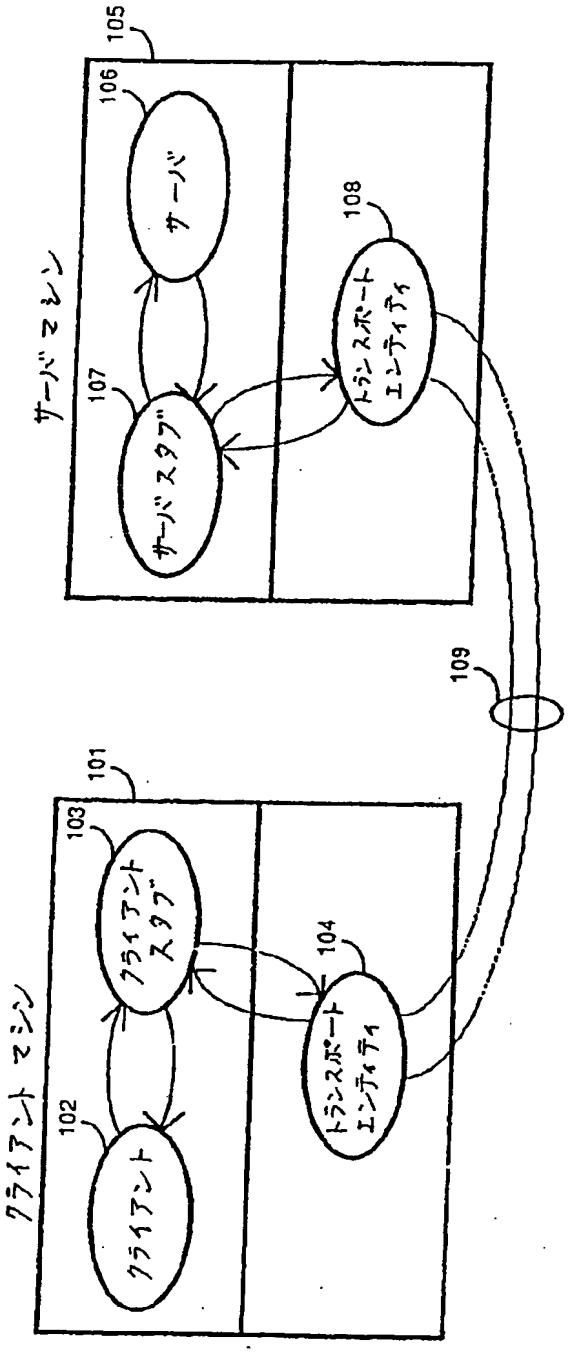
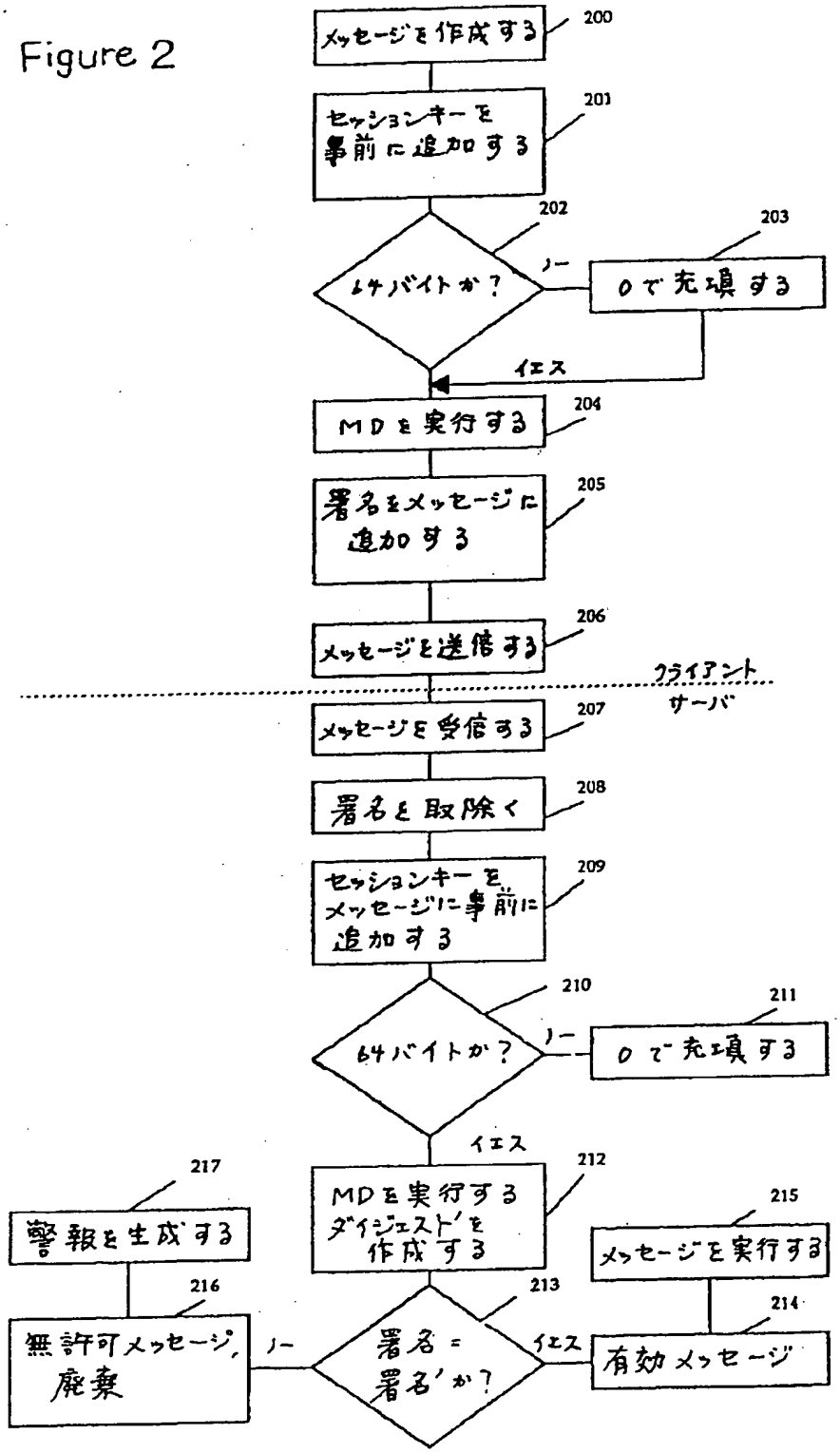

105
106
サーバ
108
トランスポート
エンティティ
サーバ マシン
107
サーバ スタブ
109
101
103
クライアント
スタブ
104
トランスポート
エンティティ
クライアント マシン
102
クライアント

Figure 1

【図２】

Figure 2


メッセージを作成する
200
セッションキーを事前に追加する
201
202
8ケバイトか？
ノー
203
0で充填する
イエス
MDを実行する
204
署名をメッセージに追加する
205
メッセージを送信する
206
クライアント
サーバ
メッセージを受信する
207
署名を取除く
208
セッションキーをメッセージに事前に追加する
209
210
64バイトか？
ノー
211
0で充填する
イエス
MDを実行するダイジェスト'を作成する
212
215
メッセージを実行する
214
有効メッセージ
213
署名＝署名'か？
イエス
ノー
216
無許可メッセージ，廃棄
217
警報を生成する

【図３Ａ】

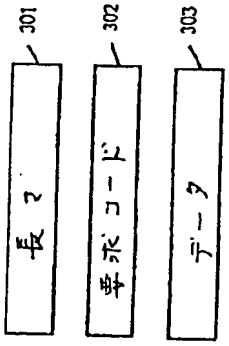



Figure 3A

【図３Ｂ】

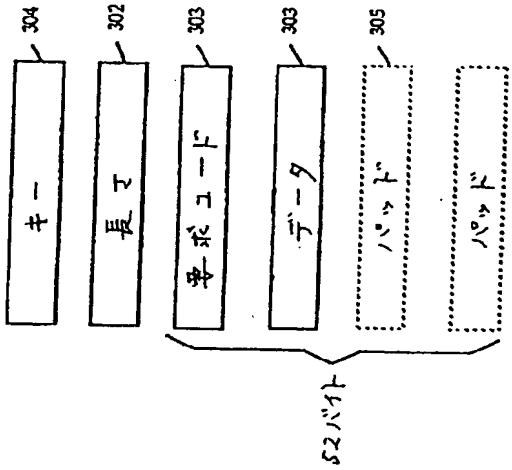



Figure 3B

【図３Ｃ】

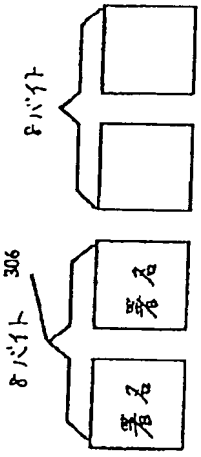



Figure 3C

【図３Ｄ】

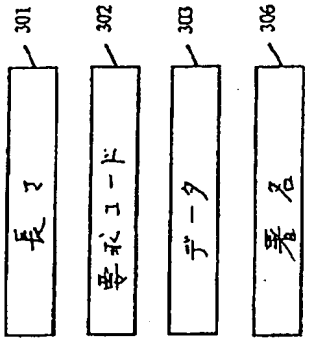



Figure 3D

【図３Ｅ】

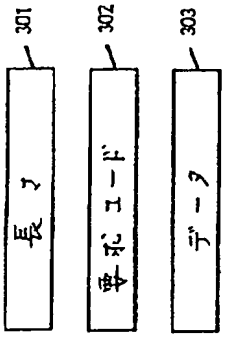



Figure 3E

【図３Ｆ】

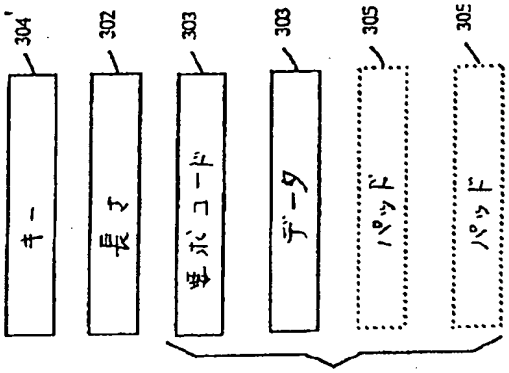



Figure 3F

【図３Ｇ】

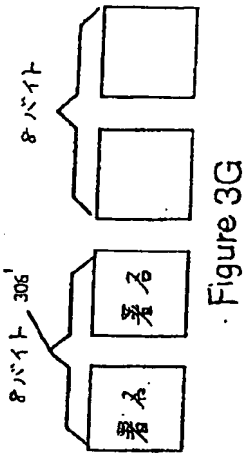



Figure 3G

【図４】

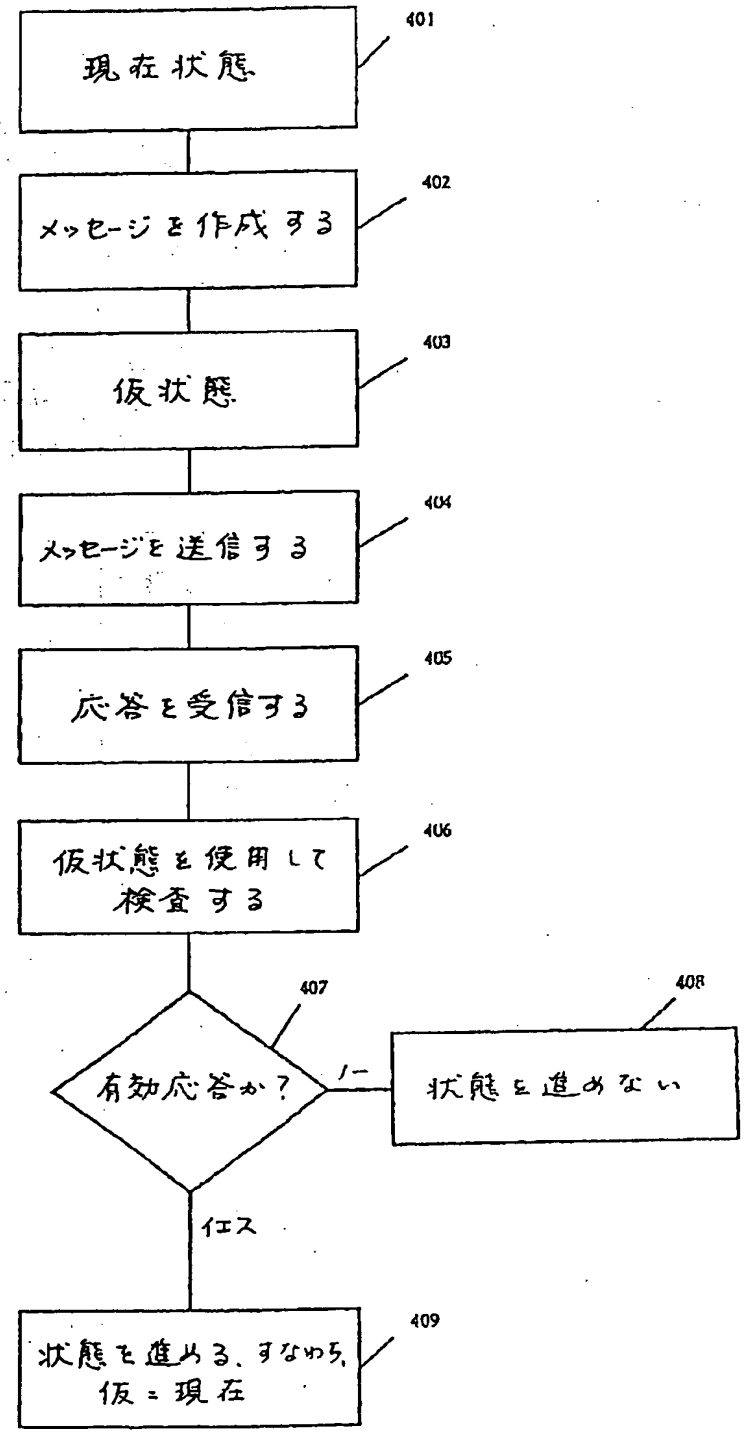

現在状態
401
メッセージを作成する
402
仮状態
403
メッセージを送信する
404
応答を受信する
405
仮状態を使用して検査する
406
有効応答か？
407
ノー
状態を進めない
408
イエス
状態を進める、すなわち仮＝現在
409

Figure 4

【図５】

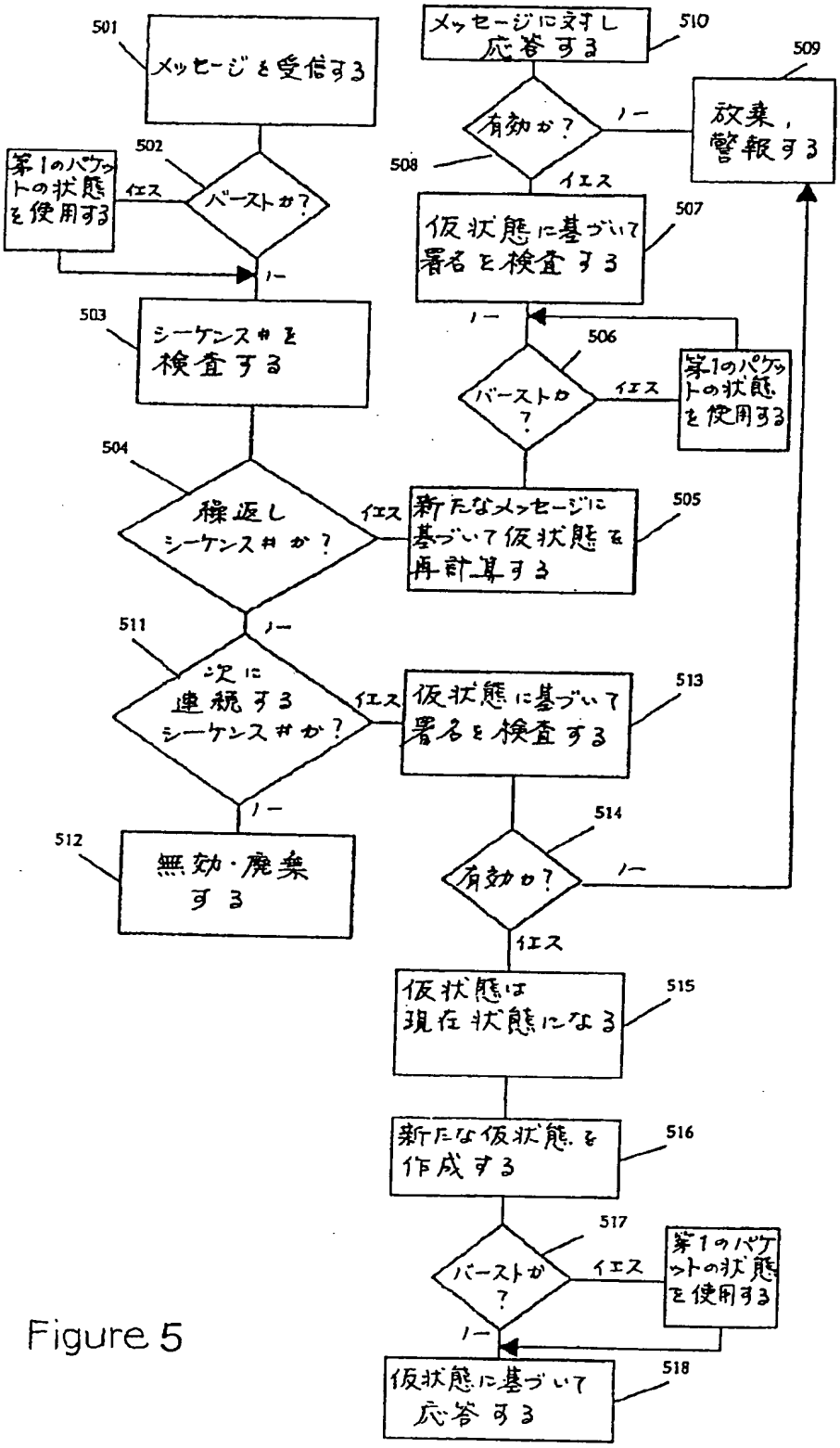

501
メッセージを受信する
502
パーストか？
イエス
第1のパケットの状態を使用する
ノー
503
シーケンス#を検査する
504
繰返しシーケンス#か？
イエス
505
新たなメッセージに基づいて仮状態を再計算する
ノー
511
次に連続するシーケンス#か？
イエス
513
仮状態に基づいて署名を検査する
ノー
512
無効・廃棄する
514
有効か？
ノー
イエス
515
仮状態は現在状態になる
516
新たな仮状態を作成する
517
パーストか？
イエス
第1のパケットの状態を使用する
ノー
518
仮状態に基づいて応答する
510
メッセージに対し応答する
509
放棄，警報する
508
有効か？
ノー
イエス
507
仮状態に基づいて署名を検査する
ノー
506
パーストか？
イエス
第1のパケットの状態を使用する

Figure 5

【図6】

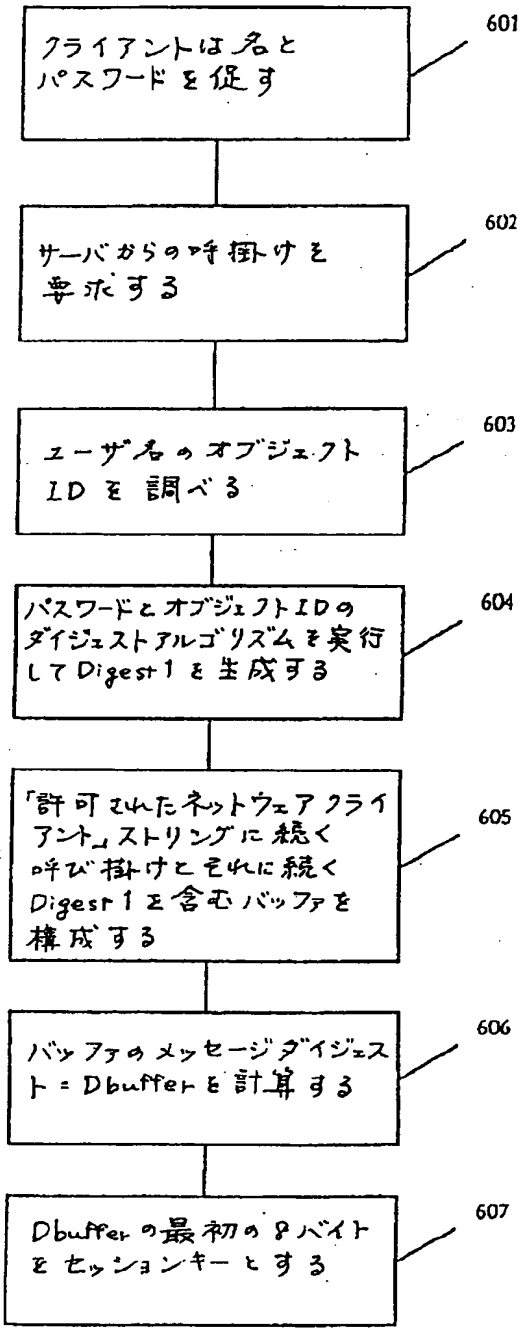

クライアントは名とパスワードを促す
601
サーバからの呼掛けを要求する
602
ユーザ名のオブジェクトIDを調べる
603
パスワードとオブジェクトIDのダイジェストアルゴリズムを実行してDigest1を生成する
604
「許可されたネットウェアクライアント」ストリングに続く呼び掛けとそれに続くDigest1を含むバッファを構成する
605
バッファのメッセージダイジェスト＝Dbufferを計算する
606
Dbufferの最初の8バイトをセッションキーとする
607

Figure 6

【図7】

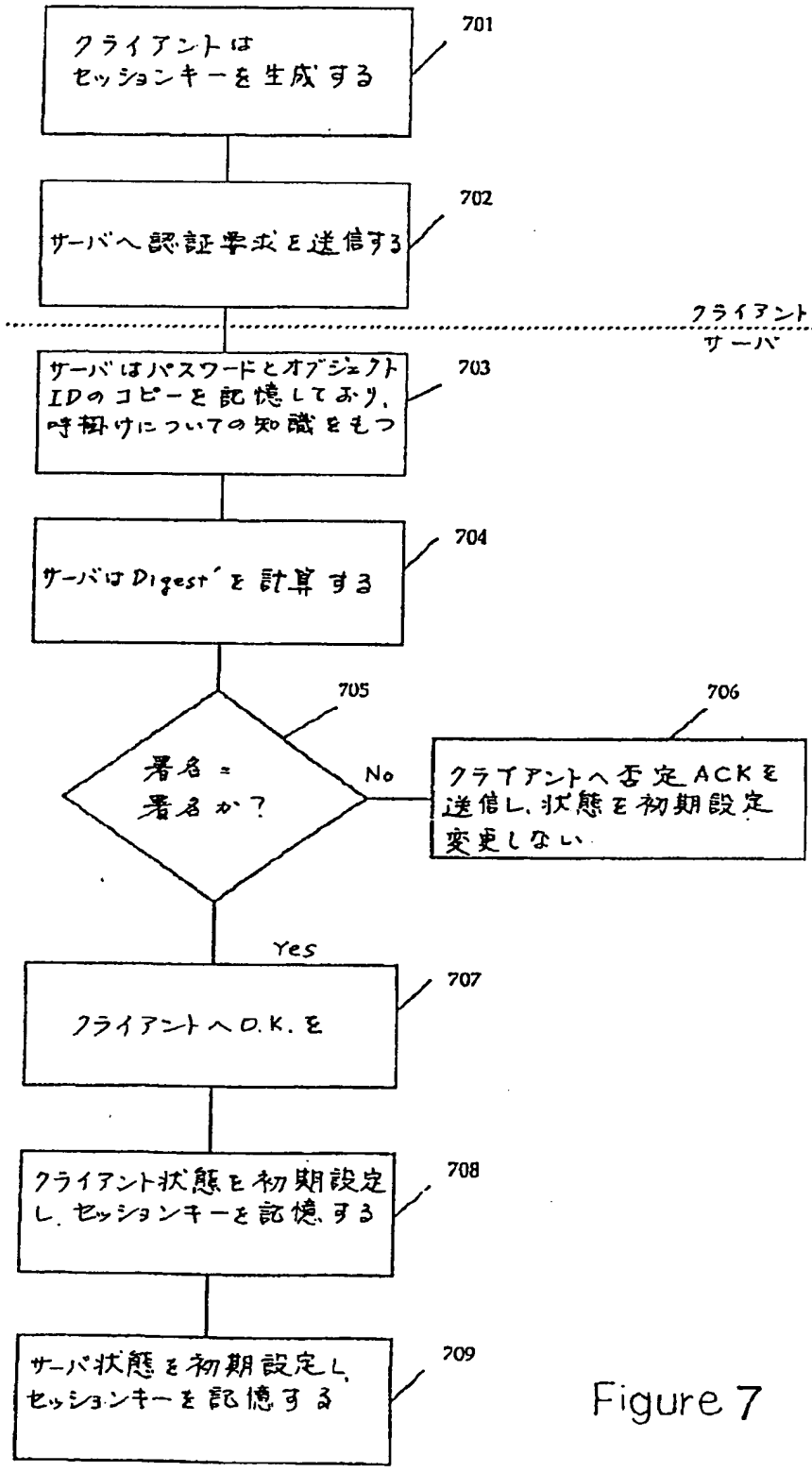

クライアントは
セッションキーを生成する
701
サーバへ認証要求を送信する
702
クライアント
サーバ
サーバはパスワードとオブジェクト
IDのコピーを記憶しており，
時刻合わせについての知識をもつ
703
サーバはDigest'を計算する
704
705
署名＝
署名か？
No
706
クライアントへ否定ACKを
送信し、状態を初期設定
変更しない
Yes
クライアントへO.K.を
707
クライアント状態を初期設定
し、セッションキーを記憶する
708
サーバ状態を初期設定し、
セッションキーを記憶する
709

Figure 7

【図８】

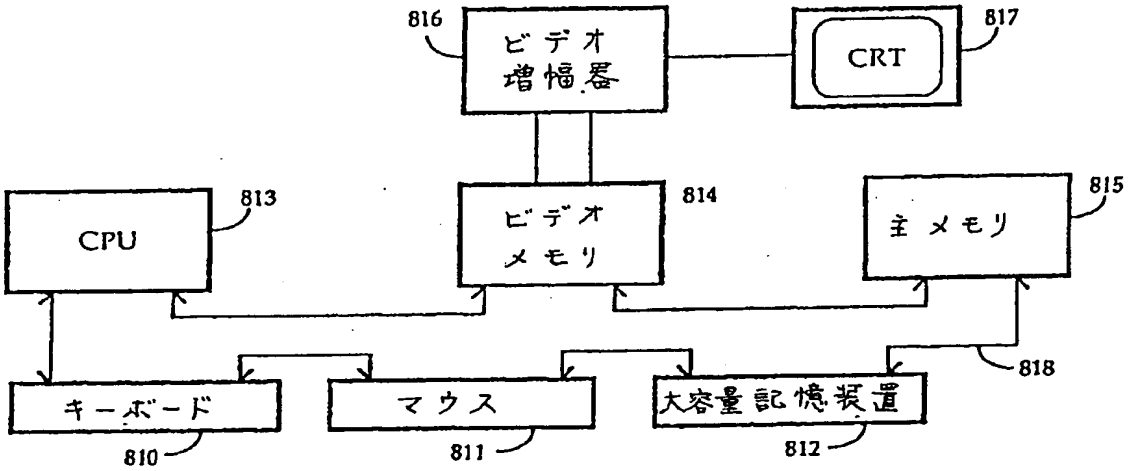

816
ビデオ
増幅器
CRT
817
CPU
813
ビデオ
メモリ
814
主メモリ
815
818
キーボード
810
マウス
811
大容量記憶装置
812

Figure 8

【図９】

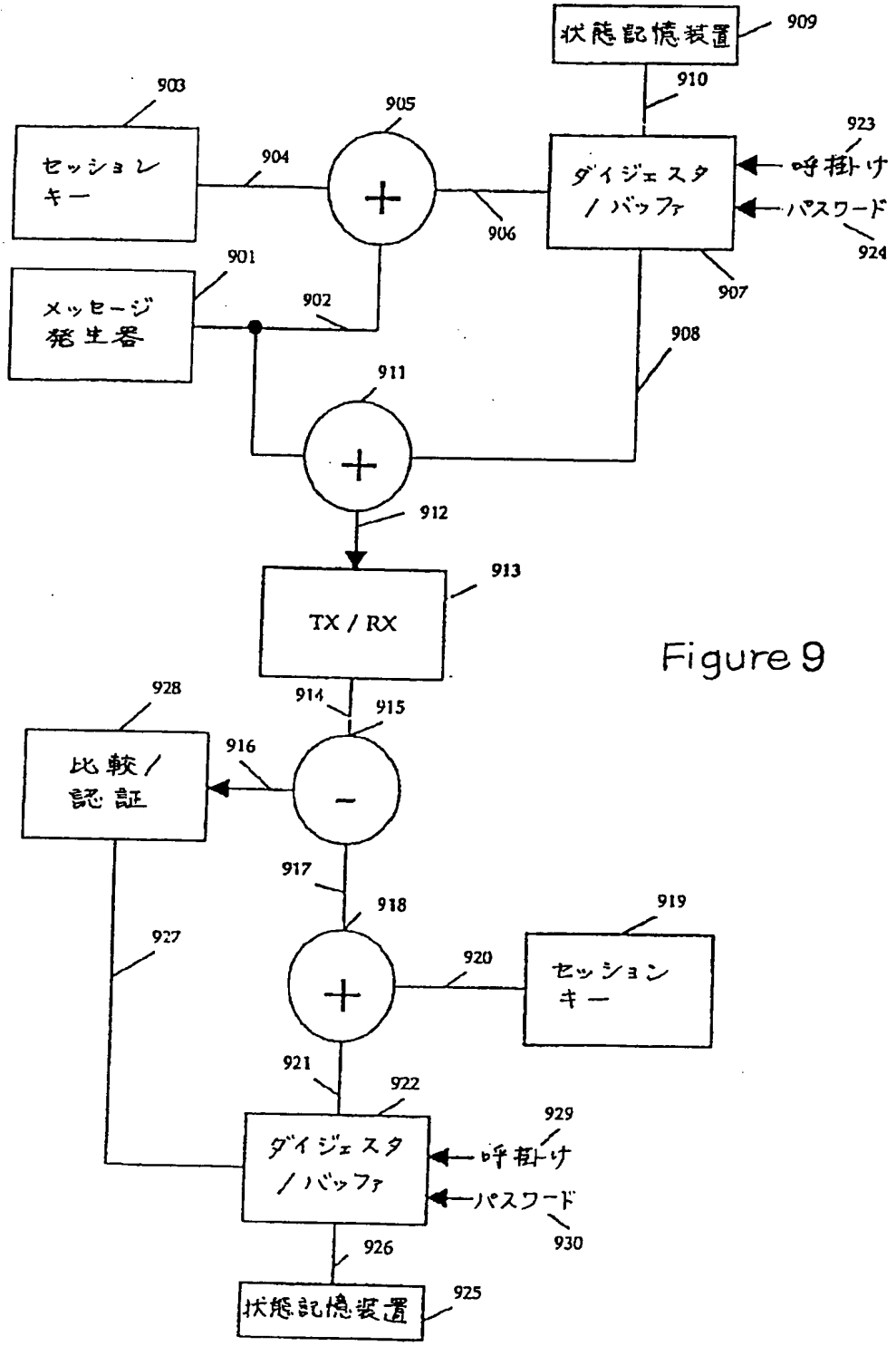

状態記憶装置
909
910
903
905
923
セッションキー
904
ダイジェスタ／バッファ
呼掛け
パスワード
906
924
901
メッセージ発生器
902
907
908
911
912
913
TX / RX
928
914
915
比較／認証
916
917
918
919
927
920
セッションキー
921
922
929
ダイジェスタ／バッファ
呼掛け
パスワード
930
926
状態記憶装置
925

Figure 9

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US93/10585

A. CLASSIFICATION OF SUBJECT MATTER
IPC(5) :H04L 9/28
US CL :380/28
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/23,25, 28, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US, A, 4,656,474 (MOLLIER ET AL ) 07 APRIL 1987, SEE ENTIRE DOCUMENT | 1-20 |
| Y | US, A, 4,799,258 (DAVIES) 17 JANUARY 1989, SEE COL. 1, LINES 50-65. | 1-20 |
| A | US, A, 4,868,877 (FISCHER) 19 SEPTEMBER 1989, SEE FIG. 5 | 1-20 |
| Y | US, A, 5,050,212 (DYSON) 17 SEPTEMBER 1991, SEE COL. 3, LINES 15-30. | 1-20 |
| Y | US, A, 5,140,634 (GUILLOU ET AL) 18 AUGUST 1992, SEE FIGS. 5 AND 6. | 1-20 |
| A,P | US, A, 5,210,795 (LIPNER ET AL.) 11 MAY 1993, SEE FIG. 2. | 1-20 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be part of particular relevance | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>13 JANUARY 1994 | Date of mailing of the international search report<br>MAR 07 1994 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>SALVATORE CANGIALOSI<br>Telephone No. (703) 308-0482 |

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA